UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/543,009	07/22/2005	Kazuya Oyama	2936-0245PUS1	1180

2292 7590 02/06/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
HAILU, TESHOME	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
02/06/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

MN

Office Action Summary	**Application No.** 10/543,009	**Applicant(s)** OYAMA ET AL.	
	Examiner Teshome Hailu	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 22 July 2005.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-39 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-39 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 July 2005 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 07/22/2005.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-39 are pending.

Specification

2. The disclosure is objected to because of the following informalities: the short form "AV" should be written as "Audio Visual" at least one time. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7, 11-26 and 30-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al (Son), US Pub. No. 2001/0017920, and further in view of Eskicioglu, US 7,039,802.

As per claims 1, 21, 26, 38 and 39 Son discloses:

An encryption code management system for use in a plurality of communication systems composed of a plurality of data processors that exchange data encrypted with specific encryption codes, (page 1, paragraph 3, the present invention relates to the field of secure video distribution networks).

Wherein there is provided an electronic apparatus including: a code management reception portion that receives the encryption codes of the data processors; (abstract, line 1-5, an encrypted form of video program received by the remote server and stored). The remote server is a distribution center acting as an intermediate device between the service provider and subscriber station.

Wherein the data processors include a code management transmission portion that transmits the encryption codes of the data processors themselves to the electronic apparatus. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server).

A code management control portion that compares a plurality of the encryption codes received by the code management reception portion; and a result output portion that outputs a comparison result yielded by the code management control portion, (abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about comparing the encryption codes received by code management reception portion and comparison result. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column 5, line 35-55, authentication of the service provider include comparing the decrypted message to the original second message sent to service provider. After authentication completed, the STB sends confirmation of this authentication back to service provider).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation and improve the quality authentication to ensure that the encrypted message was received from the desired service provider and avoid other message came form unknown sources (see column 5, line 35-40).

As per claim 2 Son discloses:

The encryption code management system of claim 1, wherein the data processors include an encryption portion that encrypts a signal transmitted from the code management transmission portion to the electronic apparatus. (Page 3, paragraph 39, first, a video program is encrypted by video on-demand source, then the encrypted program is transported to a remote server via network).

As per claim 3 Son discloses:

The encryption code management system of claim 2, wherein the electronic apparatus includes a decryption portion that decrypts the signal received by the code management reception portion from the data processors. (Page 3-4, paragraph 34, the video program, encrypted by video on-demand source and transported to remote server, decrypted by the remote server using the first key).

As per claims 4 and 23 Son discloses:

The encryption code management system of claim 2, wherein an encryption key to be used to encrypt the encryption codes is transmitted from a side that receives the encryption codes and the comparison result. (Page 3, paragraph 40, the key may be a private key of a private key encryption system. Such a private key encryption system uses a single private key to encrypt and decrypt data).

As per claims 5 and 24 Son discloses:

The encryption code management system of claim 4, wherein the encryption key used for encryption in the data processors is transmitted along with a code request signal transmitted by the electronic apparatus to request the data processors to transmit the encryption codes. (Page 3, paragraph 40, the private key(s) itself may be transmitted from the source to the server while encrypted in a second encrypted form or communication channel which is separate from the communication channel).

As per claims 6 and 25 Son discloses:

The encryption code management system of claim 2, wherein an encryption key having been used to encrypt the encryption codes is transmitted, along with the encryption codes and the comparison result, from a side that transmits the encryption codes. (Page 3, paragraph 40, the key may be a private key of a private key encryption system. Such a private key encryption system uses a single private key to encrypt and decrypt data).

As per claims 7, 15 and 16 Son discloses:

The encryption code management system of claim 1, wherein the electronic apparatus includes a code storage portion that stores one or a plurality of the encryption codes received, (page 2, paragraph 28, after the encrypted program is transported to the remote server, the remote server stored the encrypted video). Also see fig. 5A block 506.

Wherein the electronic apparatus first receives, via the code management reception portion, the encryption codes from the data processors and then stores the received encryption codes in the code storage portion, (page 2, paragraph 28, after the encrypted program is transported to the remote server, the remote server stored the encrypted video). Also see fig. 5A block 506.

Then receives, via the code management reception portion, the encryption codes from the data processors other than those corresponding to the encryption codes stored in the code storage portion, (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by the source and the encrypted program is then transported to the remote server) and (page 1, paragraph 20, the cable network typically includes one or more broadcast sources, one or more premium broadcast sources and also video on-demand). Since the cable provider has different broadcast sources, the remote server can accept different encrypted message and store them.

Then compares, in the code management control portion, the encryption codes received by the code management reception portion with the encryption codes stored in the code storage portion to search for coincidence, and then yields a search result as the comparison result.

(Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about comparing the encryption codes received by code management reception portion and comparison result. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column 5, line 35-55, authentication of the service provider include comparing the decrypted message to the original second message sent to service provider. After authentication completed, the STB sends confirmation of this authentication back to service provider).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation and improve the quality authentication to ensure that the encrypted message was received from the desired service provider and avoid other message came form unknown sources (see column 5, line 35-40).

As per claims 11 and 31 Son discloses:

The encryption code management system of claim 7, wherein the electronic apparatus includes, one for each of the data processors with which the electronic apparatus has communicated, registration keys with which to register identification codes by which the data processors are identified, and wherein the electronic apparatus stores in the code storage portion the encryption codes along with the identification codes registered with the registration keys. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server. Then the remote server stores the encrypted program).

Son does not explicitly disclose about identification codes that identifies the data processors. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column

2, line 50-60, in accordance with the present invention, the smart card includes service provider identification data associated with a plurality of service providers).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation and improve the quality authentication to ensure that the encrypted message was received from the desired service provider and avoid other message came form unknown sources (see column 5, line 35-40).

As per claims 12 and 32 Son discloses:

The encryption code management system of claim 11, wherein, in the result output portion of the electronic apparatus or the data processors, the communication systems composed of a plurality of the data processors among which the encryption codes are coincident are indicated by displaying the identification codes thereof to indicate groups to which the plurality of data processors belong. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server. Then the remote server stores the encrypted program).

Son does not explicitly disclose about identification codes that identifies the data processors. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column 2, line 50-60, in accordance with the present invention, the smart card includes service provider identification data associated with a plurality of service providers).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation and improve the quality authentication to ensure that the encrypted message was received from the desired service provider and avoid other message came form unknown sources.

As per claims 13 and 33 Son discloses:

The encryption code management system of claim 11, wherein the identification codes are installation positions and types of the data processors. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about identification codes that include types of data processors. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column 2, line 50-60, in accordance with the present invention, the smart card includes service provider identification data associated with a plurality of service providers) and (column 4, line 30-40, such identification data may include the manufacture's identification data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to ensure that the encrypted message was received from the desired service provider.

As per claims 14 and 34 Son discloses:

The encryption code management system of claim 11, wherein the identification codes are device names of the data processors. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about identification codes that include types of data processors. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column 2, line 50-60, in accordance with the present invention, the smart card includes service provider identification data associated with a plurality of service providers) and (column 4, line 30-40, such identification data may include the manufacture's identification data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to ensure that the encrypted message was received from the desired service provider.

As per claims 17 and 30 Son discloses:

The encryption code management system of claim 1, wherein, in the result output portion of the data processors or the electronic apparatus, a plurality of the data processors among which the encryption codes are coincident and that thus build one communication system are displayed as one group. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server. Then the remote server stores the encrypted program).

As per claims 18 and 35 Son discloses:

The encryption code management system of claim 1 wherein, when the encryption codes are exchanged, the encryption codes are exchanged along with device names of the data processors with which the encryption codes are associated. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Eskicioglu teach this limitation as, (column 2, line 50-60, in accordance with the present invention, the smart card includes service provider identification data associated with a plurality of service providers) and (column 4, line 30-40, such identification data may include the manufacture's identification data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Eskicioglu. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to ensure that the encrypted message was received from the desired service provider.

As per claims 19 and 36 Son discloses:

The encryption code management system of claim 1, wherein the electronic apparatus is a remote control unit for operating the data processors. (Page 2, paragraph 34, the encrypted program is transported via a primary distribution network from the video on-demand source to a remote server within a distribution center).

As per claims 20 and 37 Son discloses:

The encryption code management system of claim 1, wherein the data exchanged between the data processors is AV data. (Page 1, paragraph 3, the present invention relates to the field of video distribution networks in particular, this invention relates to secure video distribution networks).

As per claim 22 Son discloses:

The encryption code management system of claim 21, wherein the data processors include: an encryption portion that encrypts a signal to be transmitted from the code management transmission portion to the electronic apparatus; (Page 3, paragraph 39, first, a video program is encrypted by video on-demand source, then the encrypted program is transported to a remote server via network).

A decryption portion that decrypts a signal having received by the code management reception portion from the electronic apparatus, (page 2, paragraph 32, At the subscriber stations 110, the multiplexed signal is demultiplexed to isolate the re-encrypted program in the second encrypted form, the re-encrypted program is decrypted from the second encrypted form to generate the unencrypted video program, and then the video program is displayed).

Wherein the electronic apparatus includes: an encryption portion that encrypts a signal to be transmitted from the code management transmission portion to the data processors; (page 2, paragraph 31, after the video program is re-encrypted, the re-encrypted program in the second encrypted form is multiplexed with other signals to generate a multiplexed signal. The multiplexed signal is then distributed 516 via the secondary distribution network to the subscriber stations).

A decryption portion that decrypts a signal having received by the code management reception portion from the data processors. (Page 3, paragraph 34, the remote server decrypts the video program from the first encrypted form).

5. Claims 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al (Son), US Pub. No. 2001/0017920, Eskicioglu, US 7,039,802 and further in view of Garfinkle, US 5,400,402.

As per claim 8 Son discloses:

The encryption code management system of claim 7, wherein, when the electronic apparatus recognizes that a predetermined period of time has passed after the encryption codes were stored in the code storage portion, the electronic apparatus erases the encryption codes from the code storage portion. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Garfinkle teach this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Garfinkle. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

As per claim 9 Son discloses:

The encryption code management system of claim 7, wherein, when the electronic apparatus recognizes that coincidence with the encryption codes stored in the code storage portion has been found more than a predetermined number of times, the electronic apparatus erases the encryption codes from the code storage portion. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Garfinkle teach this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Garfinkle. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

As per claim 10 Son discloses:

The encryption code management system of claim 7, wherein the electronic apparatus includes an erasure operation portion that erases from the code storage portion the encryption codes stored therein. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Garfinkle teach this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Garfinkle. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to limits further access to the stored program after the limit has been reached.

6. Claims 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al (Son), US Pub. No. 2001/0017920 and further in view of Garfinkle, US 5,400,402.

As per claim 27 Son discloses

The encryption code management system of claim 26, wherein, when the electronic apparatus recognizes that a predetermined period of time has passed after the encryption codes were stored in the code storage portion, the electronic apparatus erases the encryption codes from the code storage portion. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Garfinkle teach this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Garfinkle. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

As per claim 28 Son discloses:

The encryption code management system of claim 26, wherein, when the electronic apparatus recognizes that coincidence with the encryption codes stored in the code storage portion has been found more than a predetermined number of times, the electronic apparatus erases the encryption codes from the code storage portion. (Page 2, paragraph 28, in order to generate and encrypted program in a first encrypted form, the video program is encrypted by a video on-demand source and the encrypted program is then transported to the remote server).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Garfinkle teach this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Garfinkle. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to limits further access to the stored program after the limit has been reached. (See column 2, line 19-37).

As per claim 29 Son discloses:

The encryption code management system of claim 26, wherein the electronic apparatus includes an erasure operation portion that erases from the code storage portion the encryption codes stored therein. (Abstract, line 1-5, an encrypted form of video program received by the remote server and stored).

Son does not explicitly disclose about device name of the data processors. However, on the same field of endeavor, Garfinkle teach this limitation as, (column 3, line 43-50, the stored program can be erased after a predetermined interval (e.g., 24 hours) or fixed predetermined number of accesses (e.g., one) which is fixed by data permanently stored at the customer site or specified by instructions included with the downloaded data).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Son and include the above limitation using the teaching of Garfinkle. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation to limits further access to the stored program after the limit has been reached.

Conclusion

1. The prior art made or record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: Re-encrypted delivery of video-on-demand content, US Pub. No. 2005/0097596.

TITLE: Method and system for end to end securing of content for video on demand, US Pub. No. 2004/0078575.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

January 24, 2008

***

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100